

UNITED STATES PATENT APPLICATION

OF: SCOTT KRUEGER
DANIEL GOODMAN

FOR: SECURE NETWORKED TRANSACTION SYSTEM

004437-000450

BACKGROUND OF THE INVENTION

5 The present invention relates to systems that allow debit cards, credit cards, Direct Check/ACH and other financial transaction instruments to be used in networked purchasing environments between a merchant, customer, and a third party processor. The third party processor acts as an intermediary or clearinghouse for transactions.

10 Debit cards such as those typically provided by financial institutions such as banks or credit unions require the card to be encoded or the system to be encoded to recognize the card / Personal Identification Number (PIN) combination. When used at an ATM or point of sale terminal,
15 the system contacts the financial institution or a representative thereof with the user's account number and PIN number. The account is checked to determine whether sufficient funds exist for the purchase or cash request. The system records the parameters of the transaction to make the
20 updates to the accounts such that the funds are transferred between parties of the transaction.

25 Prior art systems utilize various data encryption methods to secure the transmission of the customer's debit card/account number, customer's PIN number, the merchant's ID or code, to the various banking and transaction clearing systems that are checked at the point of sale such that an approval number is received by the merchant indicating that the transaction has been approved. The point-of-sale system
30 or a separate card reader is used to connect directly to the clearing system.

While this type of transaction allows a user to directly pay for purchases at the point of sale, it allows the potential for an unscrupulous merchant, or a party intercepting communications to have access to the user's account number and PIN number.

In an e-commerce environment, the user accesses a merchants web site, indicates the items to be purchased and is requested to supply some means to pay for the items during the checkout process. The user typically enters the credit card number and the expiration date of the card to secure the credit transaction and shipping preferences. The merchant receives this information and generates a request that is transmitted to a credit clearing system that requests approval for the purchase and transfers back an approval code to the merchant. The merchant may at this point indicates to the customer that the purchase was successful and supplies an approval page to the customer.

Since the transaction occurs over the Internet, users have concerns over the privacy and security of the information entered. These privacy and security issues limit the amount of customers that use these forms of commerce at this time. Businesses have been trying to generate more robust security mechanisms to calm nervous customers, but these system still require the customer to provide the complete billing information to the merchant to complete the sale. Robust encryption processes help to reduce the customer's anxiety to some extent.

While credit cards are commonly used in point-of sale and on-line transactions, the merchant is charged a variable fee for the transaction by the credit authorization

system based on the risk of the purchase. A higher rate for example, may be charged where the user is not at the point of sale, but is instead making the purchase at a remote location via a computer. The potential for fraud may be increased when the customer is not visible. Since the credit card company has power to act against unscrupulous merchants and to protect the consumer against fraud by merchants, customers are less concerned about the credit transaction that they would be regarding a debit transaction.

In contrast to credit purchases, there are no intermediaries to protect a customer when a debit transaction occurs. Debit transactions in contrast cause direct modifications to the clients bank account or financial assets held in a financial institution. The customer is vulnerable to direct funds transfer and withdrawal activity if someone performs these types of transactions without the customer's knowledge.

What is desired therefore is a system for allowing a customer to purchase items where the customer is not required to give the PIN number of the debit card to a merchant during an on-line purchase. It is another object of the present invention that the merchant or any party intercepting a communication between the customer and merchant, never has access to the customer's PIN number throughout the transaction. It is a further object of the present invention that all the information required to complete a transaction never exists in one transmission on the public network.

It is an object of the invention to provide a system where a third party trusted verification system is contacted during the purchase process by the merchant to request the

processing of a customer's debit transaction where the merchant only knows the card number (or a portion of it). The trusted verification system separately receives the PIN number from the customer and processes the transaction with the credit/debit processing system. The functionality performed by the trusted verification system may be performed by the debit card organization/bank directly.

SUMMARY OF THE INVENTION

The present invention, in summary form, allows a customer at a customer computing device, interacting with a merchant's computer system/web site, to buy an item with a Debit/Check or credit card. The merchant transmits details of the transaction to a trusted third party verification system (TVS) including card number, merchant number, and transaction amount. The verification system returns a transaction ID and unique verification data string to the merchant. The merchant redirects the customer to the verification system site, passing the transaction ID as part of the communications address. The verification system interacts with the user to acquire the PIN number for the debit/check card, or the expiration date and/or the CVV2 number for a credit card. Using the passed-in transaction ID and the acquired password (PIN), the verification system retrieves the merchant information from it's database, and provides the merchant number, card number, pin and transaction amount to the gateway of the Debit/Check card processing network. Upon retrieving a positive verification of the transaction success, the customer is redirected to the merchant site, passing the transaction ID and a unique verification as part of the redirection. The merchant's system compares the provided verification data string against the expected verification data string it had

earlier received from the verification system. If they match, the merchant knows the transaction was successfully completed.

Thus, in particular, in one exemplary embodiment, provided is an internetworked computer system and method having at least one user computer, at least one merchant computer, and a verification computer interconnected to a computer network such as the Internet. The computers carry out a method of approving an online transaction in conjunction with a payment card associated with the user computer. The method includes the steps of the user computer transmitting a transaction request to the merchant computer, which may include information associated with a product to be purchased by the user computer and the payment amount associated with the product. The merchant computer then transmits a verification request to the verification computer, the verification request including a first data string associated with the payment card (such as a debit card account number) and optionally an indication of a payment amount associated with the transaction request. The verification request is then stored at the verification computer in association with a transaction identifier and a verification data string, and the transaction identifier and the verification data string are transmitted from the verification computer to the merchant computer. The merchant computer stores the verification data string as an expected verification data string and the transaction identifier. The merchant computer then transmits the transaction identifier to the user computer, and the user computer transmits the transaction identifier to the verification computer. This may be accomplished by the merchant computer redirecting the web browser of the user computer to the verification computer with the appropriate data. The user computer also transmits a second data string

associated with the payment card (such as the PIN for the debit card) after being requested by the verification computer.

5 The verification computer uses the transaction identifier received via the user computer to retrieve the verification request previously stored with that received transaction identifier, and then it performs a verification step by using the first data string associated with the payment card retrieved from storage and the second data string associated with the payment card received from the user computer to verify if the transaction should be approved, e.g. by determining if an account associated with the payment card is sufficient to cover the payment amount in the verification request.

10 The verification computer will, upon successful verification that the transaction should be approved, transmit a verification approval message to the user computer, which includes the transaction identifier and the verification data string associated therewith as a confirmation verification data string, and the user computer transmits the verification approval message to the merchant computer. This may also be accomplished by the verification computer redirecting the web browser of the user computer to the merchant computer with the appropriate data. The merchant computer uses the transaction identifier in the verification approval message to retrieve an expected verification data string it had previously stored. The merchant computer then compares the expected verification data string with the confirmation verification data string from the verification approval message and indicates that the transaction has been approved if the comparison is positive.

In the case where the payment card is a debit card, then the first data string is an account number associated with the debit card and the second data string is a PIN. In the case where the payment card is a credit card, then the first data string is an account number associated with the credit card and the second data string is an expiration date or the CVV2 number.

Optionally, the verification computer determines if an account associated with the payment card is sufficient to cover the payment amount in the verification request by communicating with a gateway computer associated with an existing credit approval system.

BRIEF DESCRIPTION OF THE DRAWING

Figure 1 is a representation of the system components of the present invention;

Figure 2 is a process diagram of the method of the present invention;

Figure 3 is a representation of the front face of a debit card of the present invention;

Figure 4 a representation of the rear face of the debit card of the present invention;

Figure 5 is a representation of a prior art credit processing fields for on-line transactions;

Figure 6 is a representation of the debit card entry fields for on-line transactions of the present invention;

Figure 7 is a process step diagram of the present invention;

Figure 8 shows the icons associated with a sampling of the various debit processing network members that exist;

Figure 9 is a representation of an interface form for providing the PIN information that is delivered to a customer from the verification system.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present system will be described with regard to Figure 1, for allowing a user to make purchases at a networked e-tailer or retail location using a payment card such as a debit card or credit card. In the preferred embodiment, the customer that wishes to purchase a product may access the web site of the merchant using a web enabled device such that the customer may access a purchasing interface provided by or for that merchant. The customer would typically use a desktop computer, set top box, or any other type of device capable of communications through a network. For example, a customer from a Pentium class computer with a display, keyboard, mouse and processor executing an operating system such as Windows CE, 95, 98, MAC O/S, or Linux or Unix with a communication connection to a network such as the Internet may execute a web browser such as Internet Explorer or Netscape to access the merchant's web site. Wireless and satellite communication devices may alternatively be used by the customer to communicate with the verification system and perform steps

associated with completing the transactions associated with a purchase.

5 The merchant computer 20 may be a terminal connected to a network, a point of sale system, or a personal computer system, or server based system connected to a network that is capable of connecting to a merchant server web site. For Internet-based communications where a merchant web server is provided, the server may comprise any networked computing devices capable of serving interface programs that customers may access to indicate desired purchases. The merchant computer comprises communication means, storage means, and one or more processors to support the execution of the required processes. The merchant computer may optionally have one or more monitors, and input devices such as keyboard, mouse, and mag-stripe reader. The mag-stripe reader is also known as a card-swipe reader, or card-swipe device.

10 The verification system therefore is a networked computer system that comprises communications means for receiving requests from merchants and for communicating with customers during the purchase process. The communication means also permits the verification system to communicate with debit/credit card processing systems to process transactions for purchases. The verification system comprises memory means for retaining merchant records and customer records, and processor means for managing transactions.

15 The method of the present invention will now be described with regard to Figure 2. A customer at a customer computing device such as a user computer, interacting with a merchant's computer 20 system/web site, decides to buy an item with a payment card such as a debit/check card or credit card

40 at step 100. The user computer sends a transaction request, which will include details of the desired item such as a description and the payment price, to the merchant computer. The transaction request will also include a first data string associated with the payment card, such as the debit card number. The merchant computer 20 transmits a verification request comprising details of the transaction to a trusted third party verification computer system (TVS) 30 at step 110. The verification request will include information such as the debit card account number 42 (see Figure 3), merchant number (as determined from the merchant system) and the transaction amount. The verification computer 30 stores the verification request in association with a unique transaction identifier and verification data string that it has generated, and then returns the transaction identifier and verification data string to the merchant computer 20 at step 120. The merchant computer 20 then sends the transaction identifier to the verification computer via the user computer, for instance by issuing a redirect command to the user computer's web browser such that the user computer is redirected to the verification computer. The redirect command includes the passing of the transaction identifier that was received from the verification computer as part of the communications address (e.g. a parameter of a URL).

The verification computer receives the transaction identifier from the user computer and interacts with the user computer at step 150 to acquire the PIN number for the debit/check card 40 at step 160. That is, after receiving the transaction ID as part of the redirect, the verification computer will send a browser form to the user computer, inviting the user to enter the PIN as a second data string associated with the payment card. Using the passed-in

transaction identifier and the acquired PIN (or the expiration date and/or CVV2 if the payment card is a credit card), the verification computer retrieves the merchant information from its database 32 at steps 162 and 164, and may optionally retrieve records for the customer in a customer database 34 at step 166, and performs a verification process using the first data string, the second data string, and the transaction amount. The verification process may be performed externally by providing the merchant number, card number, PIN and transaction amount to the gateway of the Debit/Check card processing network 50 at step 170. Alternatively, the verification may be done internally if the verification computer is actually part of the credit network.

Upon retrieving a positive verification of the transaction success at step 180, the verification computer sends an approval message to the merchant computer via the user computer; i.e. the customer is redirected to the merchant computer at step 190, passing the transaction identifier and a verification data string as part of the redirection at step 200 back to the merchant computer. Alternatively, the merchant's system may receive a separate notification message from the verification system 30 with the approved transaction identifier and verification data string. The merchant's system compares the provided verification data string against the expected verification data string it had earlier received from the verification system. If they match, the merchant knows the transaction was completed.

The method derives additional security because the merchants never have enough pieces of information to complete the transaction by themselves. The security of acquiring the PIN is enhanced because the network transmission containing

the PIN never contains the corresponding card number and vice versa. Using readily available secure transmission protocols further increase security of all network transmissions.

5 This method is unique in that the merchant or any party intercepting a communication never has the customer's PIN number. It is further unique because the Debit/Check card and PIN numbers were never transmitted together during any part of the network exchanges between any of the three
10 parties.

 The debit card may be any type of debit card currently recognized by some of the present transaction service providers. The debit card typically has embossed characters 42 for the financial institution 43 and account number 44 where the characters are raised above the front of the card (see Figure 3) The most commonly quoted standards are the ISO/IEC 7810, 11, 12 and 13 series of standards. These standards are written for the credit and debit card market and so include information on the embossed characters on the cards as well as the track locations and information on the magnetic stripe that appears on the rear of the card 45. ISO/IEC 7811 has six parts with parts two and six specifically about low and high coercivity magnetic stripes. These standards include
25 information on the magnetic properties that guarantee that the stripe can be read in a magnetic stripe reader in the U.S.A. as well as in Japan. The companion to the ISO/IEC 7811 series of standard is ISO/IEC 10 373. This document details the test methods for the ISO/IEC 7811 series of standards.

30 Debit cards are preferably processed by the verification system through the existing ATM backbone of service providers. There are several different ATM backbone

networks, and many have reciprocity agreements, so one ATM can usually talk to the bank of another system. Some of the icons for the providers are displayed in Figure 8. A merchant that uses the functionality of the present system would typically be provided applets or modified HTML forms that direct the processing of debit transactions. For example, a modified form such as shown in Figure 6 would cause a transaction to be generated to contact the verification system through a first connection. Upon receiving the debit card information, the verification system may identify the appropriate ATM backbone to be contacted by interpreting the account number typed in by the customer and, or data read from the magnetic stripe of the debit card. A customer from a remote customer computer may be able to provide input to the merchant web page and the verification system using various hardware peripherals such as a mag-stripe reader or keyboard and mouse to enter the debit card number. If the customer is at a merchant location or on the merchants web site, the merchant or customer may select or choose the symbol of one of the ATM backbones indicated on the customer's card from the web page. Figure 9 shows an web page that might be used by the customer to select the ATM system and to enter the PIN number. The merchant would have a similar form with the account number and without the PIN number. In cases where the user has a card not supported by the ATM or point of sale system, extra charges may be incurred when performing transactions with a card that does not belong to the preferred system of the ATM or point of sale system. For example, one card may be a member of Exchange, Plus, Interlink and CU Access. Another Debit card may be configured as a member of Honor, Interlink, and Cirrus.

Generic card readers at merchant locations are configured to read from any type of card. Visa and Mastercard

for example, may perform analysis of the card to determine which financial institution holds the account and additionally determines the type of account. The verification system of the present invention may keep a database of card number to bank account number conversions to allow the verification system to bypass the processing steps on the Visa/MC network and go straight to the ATM backbone further reducing transaction costs to the system. For example, only the first time a customer used the verification system would the system go through the Visa, Mastercard clearinghouse. This could reduce the costs of transactions even further, enhancing profit margin or lowering costs to merchants or customers.

In the preferred embodiment, the user interface displayed on the customer's web browser upon redirect to the verification system comprises navigational buttons to allow the user to return to the merchant prior to completion of the transaction. The interface may have the icons for the various debit service ATM backbones, as shown in Figure 8 and 9, where the user may select the appropriate symbol for the transaction such that the transaction is completed with the best transaction rate for that card. If the user selects an incorrect icon or if the debit card is not supported by the system the user is informed that the transaction cannot be completed with this card. The customer may be permitted to enter another card number and account at this time if the user wishes to proceed with this transaction. The system will be able to reconcile a change in the card selected since the verification data string and transaction id are part of the current transaction. This will cause an update of the record stored in the database that was received by the TVS from the merchant.

10

45

~~20~~

25

30

5. The verification system looks up the transaction information corresponding to the transaction ID, and presents a page to the customer requesting the information to complete the transaction, such as the PIN number and optionally the

symbol representing the ATM backbone processing network,
and/or other information from the card.

5 6. The verification system forwards the combined
transaction information to the ATM backbone for completion of
the transaction.

7. The verification system gets verification /
approval from the backbone.

10 8. The customer is redirected back to the merchant
web site, passing the expected verification block to the
merchant as part of the address.

9. The merchant compares the verification block to
the one received during the initial communication with the
verification system, and if they match, knows that the
transaction was successful.

In this mode of operation, the merchant never gets
the pin. The verification system is the trusted third party
and performs the communications with the financial backbone
networks.

20 Optionally, software may be installed on the
customer's machine and run locally that will retrieve customer
information such as the PIN, and then using further
cryptography techniques, pass that information to the
25 verification system.

30 The system of the present invention may also be used
for credit card processes or any other type of transaction
where a third party (the verification server) holds part of
the transaction information. For example, where the expiration
date is held by the verification server for credit card
transactions. Another example would be where a portion of a
prepaid debit card may be provided to a third party, such that

when the card is used at a merchant location, only part of the account number is known to the merchant. The customer would provide the remainder of the account number during the verification of the second part of the transaction with the customer.

The system may be used for the monthly billing transactions for insurance companies, gas credit cards, phone bills (bells and cellular), even email from your cellphone provider. For example, your Cell-phone bill for the month of March has been mailed to address which has a link provided to the system of the present invention such as "Try our Online Direct Check payment service by going to <http://address...>".

In another embodiment of the present invention, a functionality for check processing may be provided by the system. The backend for the present verification system is also capable of doing a new Automated ClearingHouse (ACH) funds transfer process. By getting the bank routing number and account number off of a check, funds can be transferred from the customer's account do operate with checks without requiring a printed check. Some merchants currently use a process where they may handle electronic payment by check but they are actually waiting for a real check. The processing costs associated with handling paper in this way could exceed that of credit cards. By utilizing the ACH/Direct Check method from the verification server, they could significantly reduce this cost, as well as offering another payment option to entice their customers. This is by far the cheapest option in terms of transaction costs. For an insurance company, it is actually cheaper than handling paper checks.

5 An additional feature of the system may incorporate an escrow option. The money for a transaction may be held in the verification system escrow account for a specified number of days and/or the customer must confirm receiving the goods before the money is released to the merchant's account.

System Advantages

- the merchant never gets the PIN number.
- the information to complete a transaction can
10 never be intercepted by "eavesdropping" on any one channel of the communications between customer, merchant, or verification system.
- the verification system is trusted because the verification system conforms to the requirements of the different backbone processors.
- the net address of both the merchant and the customer may be held for use in fraud cases, however, the verification system would not be a party to the transaction done on behalf of the merchant.

Other Benefits Of The System

25 Many debit cards are also associated with major credit card companies in such a way that they can also be used as credit cards. We can enhance the security of using these cards for debit card transactions, by requiring that the merchant NOT request all of the numbers of the card and its expiration date, thus minimizing the possibility that the debit card can be used in an unauthorized credit card
30 transaction. This makes the cards more easily managed and more secure than typical credit card transactions. For example, a merchant cannot make an unauthorized credit card transaction without the full account number and the expiration

date. For debit card transactions this date is not required, instead the customer is the only person with enough information to respond to the query for the PIN number. The merchant never has the pieces to do a debit transaction without the user entering the pin on the verification server site.

Internet merchants are paying 2.2 to 6% to a clearinghouse organization to take credit cards over the Internet. This is referred to as the non-swiped rate (the card is not physically available to run through a terminal.) The rate is higher due to the potential for fraud. Because the present system will be able to provide the PIN number, therefore proving to a greater extent that the customer is in actual possession of the card, a more favorable processing rate can be negotiated. The system of the present invention can therefore give the merchant the chance to decrease their transaction costs.

The verification system subscribers such as preferred merchants would benefit greatly from making the distinction up front between debit and credit cards. For example, one potential customer uses a typical order page that looks like the sample shown in Figure 5. By changing the page to include a debit card field, the transactions form would look more like Figure 6. Based on the preferential physical placement of the debit card information, it would be more likely that a customer would choose the debit option. The user may benefit if part of the cost savings are passed onto them and the merchant would see a reduction in transaction costs.

5 The customer computing device may alternatively be a
device located at a retail location. For example, the user
may use their debit card at the point of sale by swiping the
card through a reader, then enter their PIN number on a
separate system that is connected with the verification system
of the present invention. The Internet-based verification
step would be executed as a separate application having no
direct connection to the merchant transaction. This would of
course require a shift in the merchant's and customer's
10 paradigm of their understanding of a point-of sale system. The
separate components may be provided to allow the customer to
establish a communication link to the verification system,
where once connected, the customer may provide the remaining
information to complete the transaction without communicating
with the point of sale system.